WHITE PAPER

proofpoint.

MACHINE-POWERED LEARNING FOR PEOPLE-CENTERED SECURITY

PROTECTING EMAIL WITH THE PROOFPOINT STATEFUL COMPOSITE SCORING SERVICE

INTRODUCTION: OUTGUNNED AND OVERWHELMED

Today's attackers are moving and adapting faster than most cyber defenses. More threats are slipping past email defenses. They're consuming more time and resources when detected—if they're detected at all. And they're talking longer to resolve.

The result: added work for already-stretched security teams, more security incidents, costlier cleanups, and greater risk to your business.

OVERCOMING THE HUMAN FACTOR

Detecting email-based threats still relies heavily on human analysis for spotting new and emerging threats. Today's attacks target people, not just technology. So this human insight is helpful, even necessary.

But traditional approaches are reaching their natural limits. They don't scale. And they can't keep up with fast-moving spam and advanced email threats.

HOW AUTOMATION CAN HELP

To keep up with today's threats, the security industry needs a new approach.

Automating email analysis can help organizations manage a growing volume of email and constantly evolving threat tactics. And it can protect against new kinds of threats such as email fraud carried out by attackers impersonating people in your organization.

To this end, Proofpoint has developed the Stateful Composite Scoring Service (SCSS). This technology helps security teams more easily deal with everything from spam and bulk mail to advanced attacks, including email fraud.

SCSS automates analysis in an integrated way. It instantly weighs a range of factors—from the email's content to its metadata to the organization's normal email flow—to determine whether the message is wanted or unwanted. And through machine learning, it recognizes patterns that helps it detect new threats faster and adjust as attackers change their tactics.

This paper explains why automation is a critical part of email security, what makes SCSS more effective than other approaches, and how it can help you stop threats and other unwanted email out of users' inboxes.

FROM SPAMMERS TO SCAMMERS: HOW TODAY'S EMAIL ATTACKS ARE CHANGING

Conventional approaches to email protection are struggling under the weight of two converging trends: a growing volume of email and harder-to-detect tactics. Spam now accounts for more than half of all email, and it's evolving quickly.

"Classic" spam has become easier to block. It's sent broadly and in high volumes, so security vendors have large sample sizes to work with.

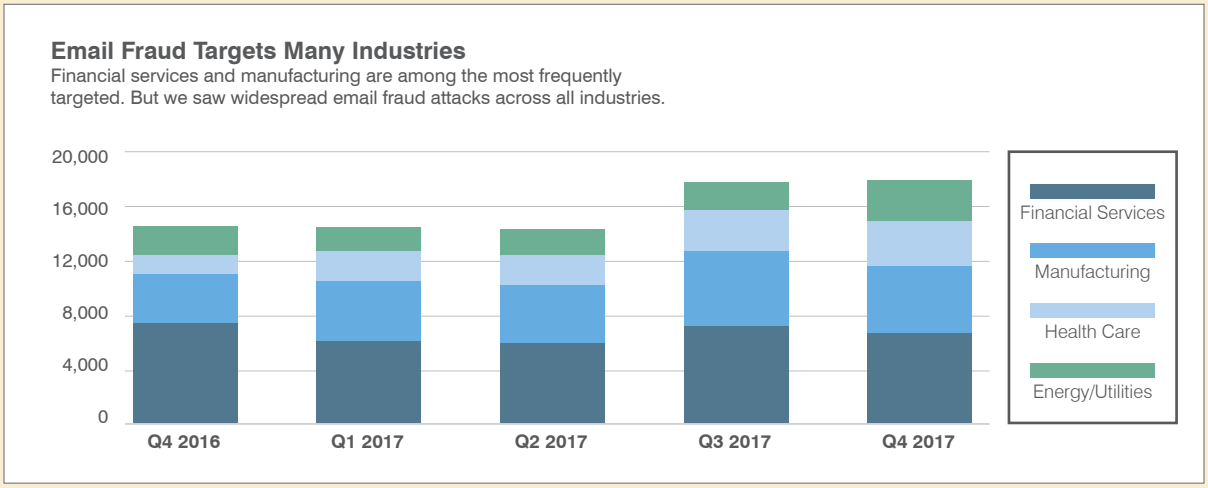
But as spam detection has improved, so have attackers' strategies. Today's spam often delivers malicious content. It is also more targeted. Rather than simply sending thousands or millions of unsafe emails—counting on a percentage of them being opened and clicked—attackers focus on a few lucrative targets.

Today's attacks spend much more time in the reconnaissance phase. Before a single email is sent, the attacker researches targeted organization, diving deep into its people and structure. Some attacks are created specifically for one organization.

EXPLOITING HUMAN NATURE WITH EMAIL FRAUD

At the same time, more attackers forgo malware attachments and malicious URLs in favor of a malware-free approach. Instead of hacking a technical vulnerability, they exploit human nature. They trick the recipient into wiring money, sending sensitive data and more.

These types of attacks are known as email fraud or business email compromise (BEC). And in pure financial terms, they are potentially much more damaging than malware. The FBI has reported over $5.3 billion in losses for companies based on these types of attacks since 2015.[1] Those are just reported losses; the actual number is likely much higher.



A WIDER RANGE OF TARGETS

While no industry is immune, email fraud is especially effective against those that have complex supply chains.

Attackers also use compromised email accounts to carry out attacks. These spoofed attacks are challenging because the email appears to be coming from a trusted source. Whaling attacks, or attacks that target an executive, are still common. But attackers use spoofing to target a wider range of people within an organization.

1 Steve Ragan (CSO). "BEC attacks have hit thousands, top $5 billion in losses globally." May 2017.

SCSS: MACHINE LEARNING FOR MORE ACCURATE SCORING

Machine learning is critical to modern email defenses. It's faster and more effective than manual analysis. And it can quickly adapt to new and evolving threats.

SCSS uses machine learning to accomplish these three things:

- Increase spam catch rates
- Give individual users a way to flag unwanted email
- Detect email fraud more effectively

Most Proofpoint customers have enabled SCSS. By aggregating threat data from this global network of deployments, SCSS uses the "wisdom of the crowd" to grow even more effective over time.

FORMING A BASELINE

In each new deployment, SCSS spends the first two weeks or so weeks examining all emails to learn the organization's normal flow. It typically analyzes thousands of emails during that period. (It also uses an aggregate baseline from hundreds of other Proofpoint deployments to account for spam that may already be part of the organization's email flow.)

Having this baseline allows the system to quickly spot and block email that falls outside of the norm, boosting its overall effectiveness. SCSS scores all emails using a variety of methods including:

- Machine learning for composite scoring
- Algorithmic evaluation
- Traditional scoring

These capabilities can increase overall spam effectiveness by as much as 5%. Because SCSS doesn't rely on human-produced rules, it can quickly detect and block new spam campaigns as they emerge.

SCORING SPAM, EMAIL FRAUD AND OTHER THREATS

SCSS performs deep analysis of the email's contents and context assess whether it falls within the organization's baseline. It scores on 16 distinct criteria, including traits shown in Figure 2.

SCSS doesn't simply look at bad email; it also analyzes legitimate email so that end users get all the email they want.

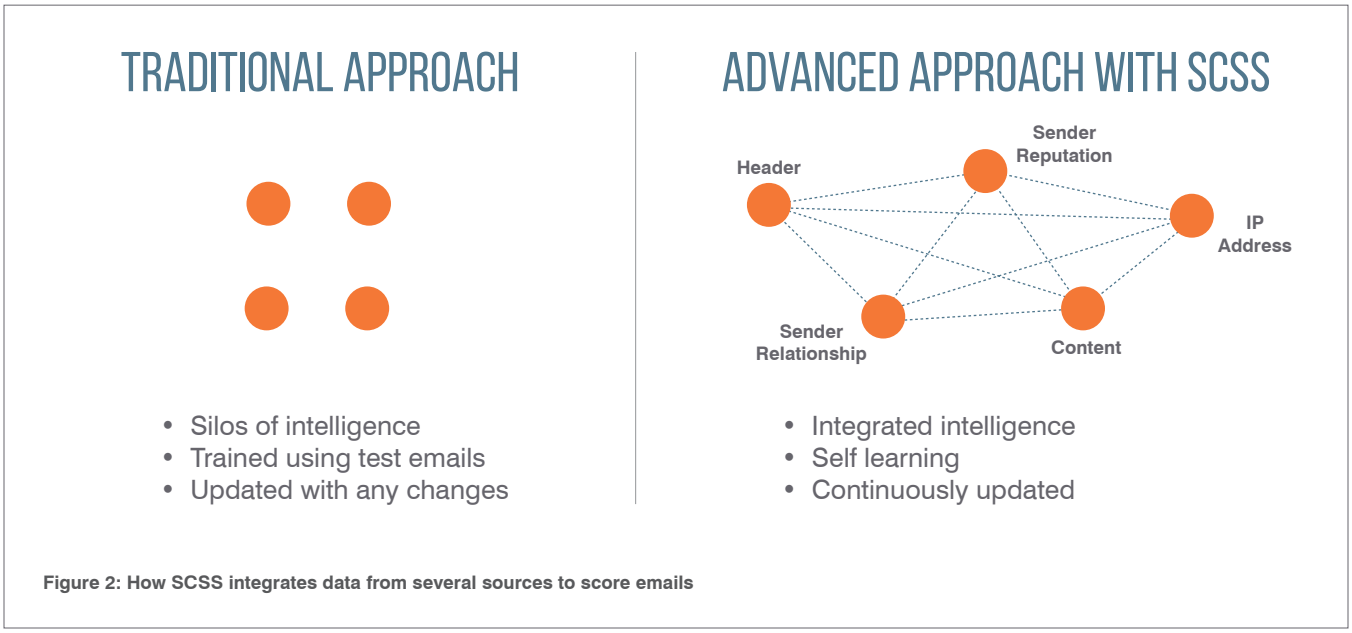


Figure 2: How SCSS integrates data from several sources to score emails

Here's how SCSS scoring works:

1. Each email received is hashed into 3-kilobyte segments.
2. Each of these segment is scored.
3. The scores are combined to create a composite reputation score for the email.
4. This composite reputation score determines whether the email will be delivered to the intended recipient.

This approach is especially effective at detecting email fraud. Email fraud, in which an attacker poses as someone the recipient knows or expects to do business with, is a pressing concern for customers. These impostor emails are highly targeted and don't contain malware. So traditional email security tools often fail to detect them.

This integrated analysis helps SCSS detect email fraud that uses reply-to spoofing. (In reply-to spoofing, the email shows the name of and email address of a real executive or partner. But the Reply-to address—where any replies are actually sent—is the attacker's.)

SCSS can also block emails with spoofed domains. (In this type of email fraud, the attacker uses a trusted domain to pose as someone within the recipient's organization or as a business partner.)

PERSONALIZING THE EXPERIENCE

Email doesn't have to be overtly malicious to be unwanted. Your users may object to marketing emails, newsletters, and other bulk mail that clutter up their inboxes. In the past, filtering them required an email administrator to step in and help.

With SCSS, users themselves can mark emails they want or don't want. SCSS learns from this feedback to intelligently provide only emails they want to see. This feedback also informs our global classification engine to make email filtering even more intelligent. Users get more control over their inbox and a better email experience.

CONCLUSION AND RECOMMENDATIONS

Stopping advanced email threats is more critical than ever. More than 90% of targeted attacks arrive through email. Blocking them before they enter your environment—where they already have a foothold and are doing damage—is the most effective way to protect your organization.

Conventional tools and strategies can go only so far against email attacks. SCSS is a new approach.

Using automation, machine learning, and a large, integrated set of email data, SCSS is highly effective at stopping unsafe and unwanted email—and making sure that users get the email they do want.

To learn more about how Proofpoint can
help you protect your people,

proofpoint.com/us/product-family/email-protection

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint.

www.proofpoint.com

0318-030